Abstract of CN1440604

Embedded hardware of the present invention is optimized to perform packet or cell filter function by receiving packet or cell from the external and internal network, network address conversion function, and access control function and TCP connecting control function. A general-purpose computer coupled with the embedded hardware via the PCI interface executes various functions as a firewall of certification etc. for user under the general Windows operation system as an application program. In accordance with the present invention, packet or cell filter function, etc. which is the essential function of the firewall adopts to copes with the speed of the network communication becoming more and more fast with high speed process in the embedded hardware, and to carry out various functions corresponding to the standards approved by the government so that expansion of functions and diversity can be obtained.

[19] 中华人民共和国国家知识产权局

[51] Int. Cl⁷
H04L 12/22
G06F 11/00

[12] 发明专利申请公开说明书

[21] 申请号 01812268.X

[43] 公开日 2003 年 9 月 3 日

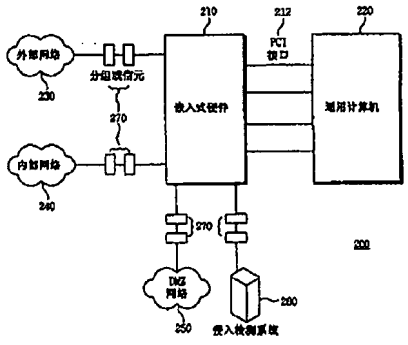
[11] 公开号 CN 1440604A

[22] 申请日 2001.7.3 [21] 申请号 01812268.X
[30] 优先权
[32] 2000. 7. 3 [33] KR [31] 2000/37622
[86] 国际申请 PCT/KR01/01133 2001.7.3
[87] 国际公布 WO02/07384 英 2002.1.24
[85] 进入国家阶段日期 2003.1.3
[71] 申请人 智谋有限公司
地址 韩国汉城市
[72] 发明人 李学茂 韩淑媛
[74] 专利代理机构 中原信达知识产权代理有限责任公司
代理人 关兆辉 张天舒
权利要求书 2 页 说明书 8 页 附图 4 页

[54] 发明名称 结合嵌入的硬件和通用计算机的防火墙系统

[57] 摘要

本发明的嵌入式硬件被最佳化以通过从外部和内部网络接收的分组或信元来执行的分组或信元过滤功能、网络地址转换功能、访问控制功能和 TCP 连接控制功能。根据作为一个应用程序的通用视窗操作系统，经 PCI 接口与嵌入式硬件耦合的通用计算机执行用于用户的作为一个认证的防火墙的各种功能等等。按照本发明，分组或信元过滤功能等等，在嵌入式硬件中这都是防火墙的基本功能，适于应付随着高速处理变得越来越快的网络通信速度，并执行对应于由政府批准的标准的各种功能以便能够获得扩展的功能和多样性。



ISSN1008-4274

知识产权出版社出版

1. 一种防火墙系统，用于防止来自外部和内部网络的未授权的网络侵入，包括：

嵌入式硬件，它被设计从所述外部和内部网络接收分组或信元和完成作为防火墙的第一功能；和

通用计算机，它被连接到所述嵌入式硬件，并被编程以完成不同于作为一个防火墙的所述第一功能的第二功能。

2. 按照权利要求 1 的防火墙系统，其中由所述嵌入式硬件完成的所述第一功能包括：

分组或信元过滤功能，从所述外部和内部网络接收分组或信元，并选择性的在网络间传送或阻止所述分组或信元；

网络地址转换功能，重新的定义内部网络的 IP 地址；

访问控制功能，限制网络间分组或信元的访问；和

TCP 连接管理功能，在网络间通过 TCP 协议保持一个连接。

3. 按照权利要求 1 的防火墙系统，其中由所述通用计算机完成的所述第二功能包括用户验证功能，用于识别和验证试图访问的用户的身份。

4. 按照权利要求 1-3 的任一权利要求所述的防火墙系统，其中所述嵌入式硬件和所述通用计算机是经过 PCI 接口彼此连接的。

5. 一种防火墙系统，用于防止来自外部和内部网络的未批准的网络侵入，包括：

通用计算机，从所述外部和内部网络接收分组或信元；和

嵌入式硬件，它被连接到所述通用计算机，并被设计完成作为防火墙的第一功能，

其中所述通用计算机被编程以完成不同于作为一个防火墙的所述

第一功能的第二功能。

6. 按照权利要求 5 的防火墙系统，其中由所述嵌入式硬件完成的所述第一功能包括：

分组或信元过滤功能，选择性的在网络间传送或阻止所述分组或信元；

网络地址转换功能，重新的定义内部网络的 IP 地址；

访问控制功能，限制网络间分组或信元的访问；和

TCP 连接管理功能，在网络间通过 TCP 协议保持一个连接。

7. 按照权利要求 5 的防火墙系统，其中存储在所述通用计算机中的所述第二功能包括用户验证功能，用于识别和验证试图访问的用户的身份。

8. 按照权利要求 5-7 的任一权利要求所述的防火墙系统，其中所述嵌入式硬件和所述通用计算机是经过 PCI 接口彼此连接的。

结合嵌入的硬件和通用计算机的防火墙系统

发明领域

本发明涉及用于在网络上阻止塞侵入的一种防火墙系统，并尤其涉及结合嵌入的硬件和通用计算机所配置的一种防火墙系统，并提供更大的效率和高速性能。

相关技术的描述

直接针对于在因特网上防止来自外部的或内部的网络的未授权的网络侵入的一个防火墙被定位在网络的连接点之间，并完成控制和监督管理通过该网络的所有网络连接的作用。

图 1 是一个普通防火墙系统的一个网络结构图。

通常，防火墙 40 被建立在内部网络 10、外部网络 20、DMZ 网络 30 和侵入检测系统 60 之中，并处理通过网络之间的一个分组或信元以便控制其中的访问。防火墙 40 通过路由器 50 和外部网络 20 连接，并且网服务器 70 和邮件服务器 80 被连接到 DMZ 网络 30。存在 DMZ 网络 30 以便在内部网络 10 中对外部网络 20 提供开放的服务。此外，侵入检测系统 60 执行检测已经访问网络的一个用户的动作的功能，和按照用户的动作，确定是否该用户是具有侵入目的的一个黑客，并连同防火墙 40 被链接完成阻止侵入的功能。

这样常规的防火墙系统能被分成两种形式。

第一种常规防火墙系统被实施成一个专用硬件。换句话说，第一种专用的防火墙是包括一个 CPU 的专用硬件，它被设计完成只作为一个防火墙，一个存储器，一个网络接口等等的功能。

同时，第二种常规防火墙系统被实施成基于视窗操作系统的通用计算机。就是说，执行防火墙功能的一个程序被存储在诸如通用计算机的存储器中，能够使 CPU 完成该功能。

这样的第一和第二常规防火墙系统具有它们各自的问题。

第一种常规防火墙系统实施成专用硬件，尽管优点在于设计它加快了一个具体操作，从而它的高速处理是可能的，但是因为它是一种专用硬件各种功能的扩展受到限制。而且，在由政府批准的观察评估等级中包括专用硬件的防火墙系统具有困难。此外的缺点是，对于不具有相关技术知识的一个人来说，实施这样的专用硬件的防火墙系统是困难的。

第二种实施成通用计算的常规防火墙系统的优点在于，提供用户防火墙系统的各种功能和易于操作，即使是一个不具有相关技术知识的人。然而，因为这样的通用计算机没有被最佳的设计以处理防火墙的具体功能，无论如何提高 CPU 的性能，它的处理速度受到约束。特别的是，随着未来的时间发展，防火墙的所需要的处理量和处理速度将被增加，这就使通用计算机不能满足要求。

发明概述

直接针对克服上述现有技术的问题，本发明提供一种结合有专用硬件和通用计算机的优点的防火墙系统。换句话说，需要高速处理的防火墙的一个分组或信元过滤功能等等，这些防火墙必不可少的功能提前在专用硬件中被快速处理，并且对应于政府批准的标准的各种功能在通用计算机中被处理。

为了实现上述目的，本发明提供了一种防火墙系统，用于防止从外部或内部网络的未授权的网络侵入，该系统包括嵌入式硬件，其被

设计用于从外部或内部网络接收一个分组或信元和执行作为防火墙的第一种功能，并将通用计算机连接到嵌入式硬件，以及编程来执行作为一个防火墙的不同于第一种功能的第二种功能。

就此而论，由嵌入式硬件完成的第一种功能包括从外部或内部网络接收一个分组或信元的分组或信元过滤功能，并在网络之间选择性的传送和阻止所述分组或信元，一个网络地址变换功能重新定义内部网络的 IP 地址，一个访问控制功能，限制网络之间分组或信元的访问，和一个 TCP 连接管理功能，在网络之间通过 TCP 协议保持一个连接。

此外，由通用计算机完成的第二种功能包括：用户验证功能，识别和验证试图访问的用户的身份。并且，期望经过 PCI 接口彼此连接嵌入式硬件和通用计算机。

为了实现上述目的，本发明提供一种防火墙系统，用于防止来自外部的或内部网络的未授权的网络侵入，其包括从外部或内部网络接收一个分组或信元的通用计算机，和被连接到通用计算机的嵌入式硬件，并且被设计完成作为防火墙的第一功能，其中通用计算机被编程以完成不同于作为防火墙第一功能的第二功能。

就此而论，通过嵌入式硬件完成的第一功能包括：在网络之间选择性的传送或阻止分组或信元的分组或信元的过滤功能，一个网络地址转换功能，重新定义内部网络的 IP 地址，一个访问控制功能，限制网络之间一个分组或信元的访问，和一个 TCP 连接管理功能，在网络之间保持连接到 TCP 协议。

另外，由通用计算机完成的第二功能包括：用户验证功能，识别和验证试图访问的用户的身份。并且，期望经过 PCI 接口彼此连接嵌入式硬件和通用计算机。

简述附图

图 1 是一个通用防火墙系统的网络结构图。

图 2 是一个方框图，表示根据本发明第一优选实施例的嵌入式硬件的构造。

图 3 是一个方框图，表示根据本发明第一优选实施例的防火墙系统的构造。

图 4 是一个方框图，表示根据本发明第二实施例的防火墙系统的构造。

优选实施例的详细说明

在下文中，参考在此的附图特别解释本发明的优选实施例。

图 2 是一个方框图，表示按照本发明第一优选实施例的嵌入式硬件的结构。在此，嵌入式硬件表示被最佳设计的专用硬件以完成只作为一个防火墙在高速上的具体功能。

嵌入式硬件 100 包括 CPU102，RAM104，ROM106，存储管理信元 108，LED 控制器 110，电源管理信元 112，通信协议接口 114，PCI 总线接口 120，以太网或 ATM 接收接口 130，和以太网或 ATM 发送接口 132。

基于简单算法 CPU102 执行需要高速处理的运算，这是一个防火墙系统功能中必不可少的，并控制嵌入式硬件 100 的所有操作。这样，在 CPU 中处理多数的简单运算，从而几乎不影响整个硬件系统的资源。

ROM106 存储对于防火墙系统必不可少的算法，通过操作员和本身产生的列表所设置的环境值。该算法、环境值和列表被用于快速访问处理到 CPU102。

PCI 总线接口 120 被安置在通用计算机 140 的 PCI 槽上，并且当

操作时，起到嵌入式硬件 100 和通用计算机 140 的一个接口的作用，以便它们能彼此互补侵入阻止功能。该 PCI 总线接口 120 能容易的安装在建立的计算机系统中和被使用，而不用在硬件结构中做任何改变。

以太网或 ATM 发送/接收接口 130 和 132 是内部网络 10，外部网络 20，DMZ 网络 30，和图 1 的侵入检测系统 60 的接口，它能够使以太网分组或 ATM 信元在网络 150 之间被发送。

通信协议接口 114 起到在通用计算机的基于视窗操作系统的应用程序和嵌入式硬件 100 的操作系统之间进行通信的作用。在用户通过使用应用程序改变环境值和把一个确定值传送到嵌入式硬件 100 中的应用程序的情况下，它通信并能够使两个系统被共同链接。

如上所述，嵌入式硬件 100 被最佳的设计以便只执行在防火墙中特殊的和必不可少的功能（将在后面的图 3 中解释），因而提供高速和高性能的功能。此外，完成上面功能的嵌入式硬件 100 不必具有与图 2 所示的相同的结构。并且对本领域普通技术人员显而易见的是，可以作出各种可能的实施的装置，例如，一个集成芯片的实施例。

图 3 是一个方框图，表示按照本发明的第一优选实施例的防火墙系统的结构。

按照本发明第一优选实施例的防火墙系统 200 包括：发送/接收一个分组或信元 270 的嵌入式硬件 210，它与外部网络 230，内部网络 240，DMA 网络 250，和侵入检测系统 260 构成网络状的，并且通用计算机 220 通过 PCI 接口 212 与嵌入式硬件 210 连接。

在这点上，经以太网或 ATM 发送/接收接口嵌入式硬件 210 与网络连接，但通用计算机 220 不直接与网络相连接。而是通过 PCI 接口 212，AGP 或 USB 接口，将嵌入式硬件 210 和通用计算机 220 连接。

在下文中，将分别解释按照本发明第一优选实施例的防火墙系统200的嵌入式硬件210和通用计算机220的作为一个防火墙完成的它们的各自的功能。

通过嵌入式硬件（210）完成的四个功能包括：（a）分组或信元过滤功能，其中接收在网络间被传送的分组或信元并从那里获得所需要的信息，从而选择性的传送或阻止网络间的分组或信元；（b）访问控制功能，在基于网络间分组或信元的访问控制列表的规则下限制访问；（c）TCP连接管理功能，当连接是通过使用网络间的TCP协议时保持一个连接；和（d）一个网络地址转换功能，重新的定义和使用内部网络的IP地址，从而完全的阻止从外部网络到内部网络访问并解决IP地址的不足。

通过这样的嵌入式硬件210完成的上述功能应该是作为防火墙完成的功能中最频繁的和以高速的处理的功能，对于诸如防火墙的处理速度等等来说它是最核心的部分。本发明在最佳的专用硬件中完成这样频繁的和必不可少的功能，因而嵌入式硬件210，对于常规防火墙系统具有一种优良的性能。

接下来，通过通用计算机220作为一个防火墙完成可能的各种功能，例如包括，但不限于此：（a）用户验证功能，识别和验证试图访问内部或外部网络的主机的用户的身份；（b）管理员告警功能，其中一旦出现进入网络的侵入，它被快速的通知到网络安全管理员；（c）业务统计功能，通过时间，协议类型，访问类型等等，分析网络间传送的分组或信元；（d）数据集成功能，其中一旦对于有关安全功能的数据出现一个未授权的用户的非法更改而不是一个许可的管理员的正常更改，它将被察觉到和被通知给管理员；（e）审计记录功能，根据信息保护系统记录有关安全的的活动和分析记录的内容，从二防止侵入和跟踪非法行动；和（f）用户接口功能，能够使一个操作者安装防

火墙，设置和更改环境值，检查审计记录等等。

作为一个防火墙完成上面功能的装置以一种应用程序的形式被存储在基于视窗操作系统的通用计算中。就此而论，举例建议的作为一个防火墙的功能不必是必不可少的，但应遵照由政府批准的评估等级，和符合操作者的各种要求。

因此，上面的功能不必被始终地完成，并且嵌入式硬件 210 只能在操作防火墙的时间上按照操作者的决定而工作。而且，上述功能的实现是通过使用基于视窗操作系统的应用程序来实现的，该系统对于操作者是熟悉的和熟知的，以至于即使是对于不具有相关技术知识的一个人来说，也是很容易实施和操作具有上述各种功能的防火墙系统。

按照本发明第二优选实施例的防火墙系统，但与本发明的第一优选实施例相比较，所实现的目的和作用是相同的，除了结构有稍微的不同。

图 4 是一个方框图，表示按照本发明第二优选实施例的防火墙系统的结构。

按照本发明第二优选实施例的防火墙系统 300 包括：发送/接收分组或信元 370 的通用计算机 320，它与外部网络 330，内部网络 340，DMA 网络 350，和侵入检测系统 360 构成网络状的，并且嵌入式硬件 310 经 PCI 接口 312 与通用计算机 320 连接。

比较第一优选实施例的防火墙系统 200，不同处在于在第二优选实施例的防火墙系统中通用计算机负责从网络接收一个分组或信元。换句话说，通用计算机 320 经以太网或 ATM 发送/接收接口与网络连接，但嵌入式硬件 310 不直接与网络连接。这样，本发明第二优选实施例的嵌入式硬件 310 不需要在硬件中的以太网或 ATM 发送/接收接口 130

和 132，这不同于图 2 所示的嵌入式硬件 100。另外，嵌入式硬件 310 被安装在通用计算机 320 的 PCI 槽上。

在从网络接收一个分组或信元的构成中，按照第二实施例的该防火墙系统 300 不同于按照第一实施例的防火墙系统 200。然而，第二实施例的通用计算 320 和嵌入式硬件 310 所完成的作为一个防火墙的功能是与第一实施例的通用计算机 220 和嵌入式硬件 210 相同的。因此，在按照第二优选实施例的防火墙系统 300 中，嵌入式硬件 310 负责所需的频繁的和高速的处理功能，而通用计算机 320 则负责除了该功能之外的各种功能。

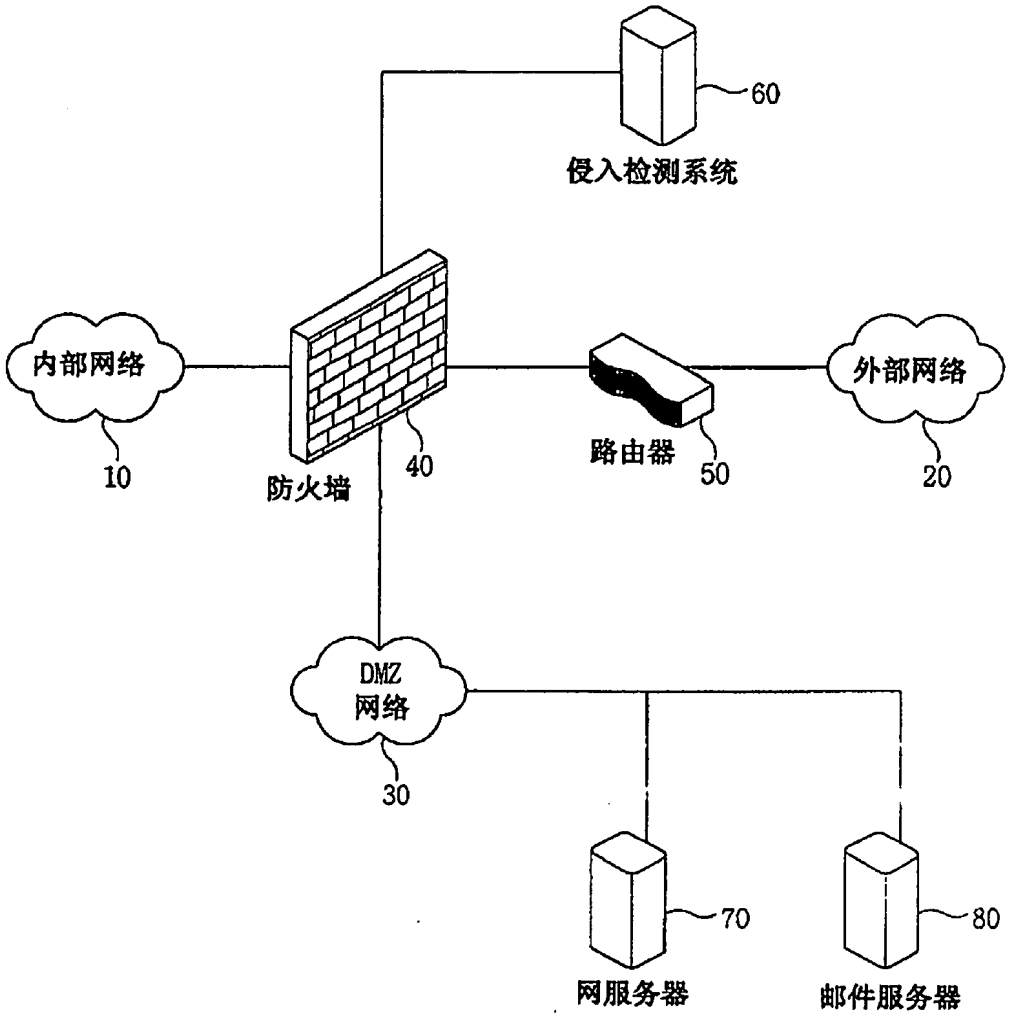
参考上面的优选实施例特别的示例和描述了本发明，然而，它们是被用于举例，并且本领域普通技术人员应该明白，在不脱离定义在所附权利要求的本发明的精神和范围下，本发明适于各种可能的修改。

工业实用性

如前所述，本发明在嵌入式硬件中以高速处理一个分组或信元过滤功能等等，是防火墙的必不可少的功能，从而适于已经变得很快的网络通信速度，并且对应于在通用计算机中由政府批准的标准的各种功能，从而获得功能的一个扩展和多样性。

此外，高性能的嵌入式硬件和提供各种功能的基于视窗操作系统的应用程序接口，能够促进用于限制特殊领域的安全装备的普及。

图1


60
侵入检测系统
内部网络
10
防火墙
40
路由器
50
外部网络
20
DMZ
网络
30
70
网服务器
80
邮件服务器

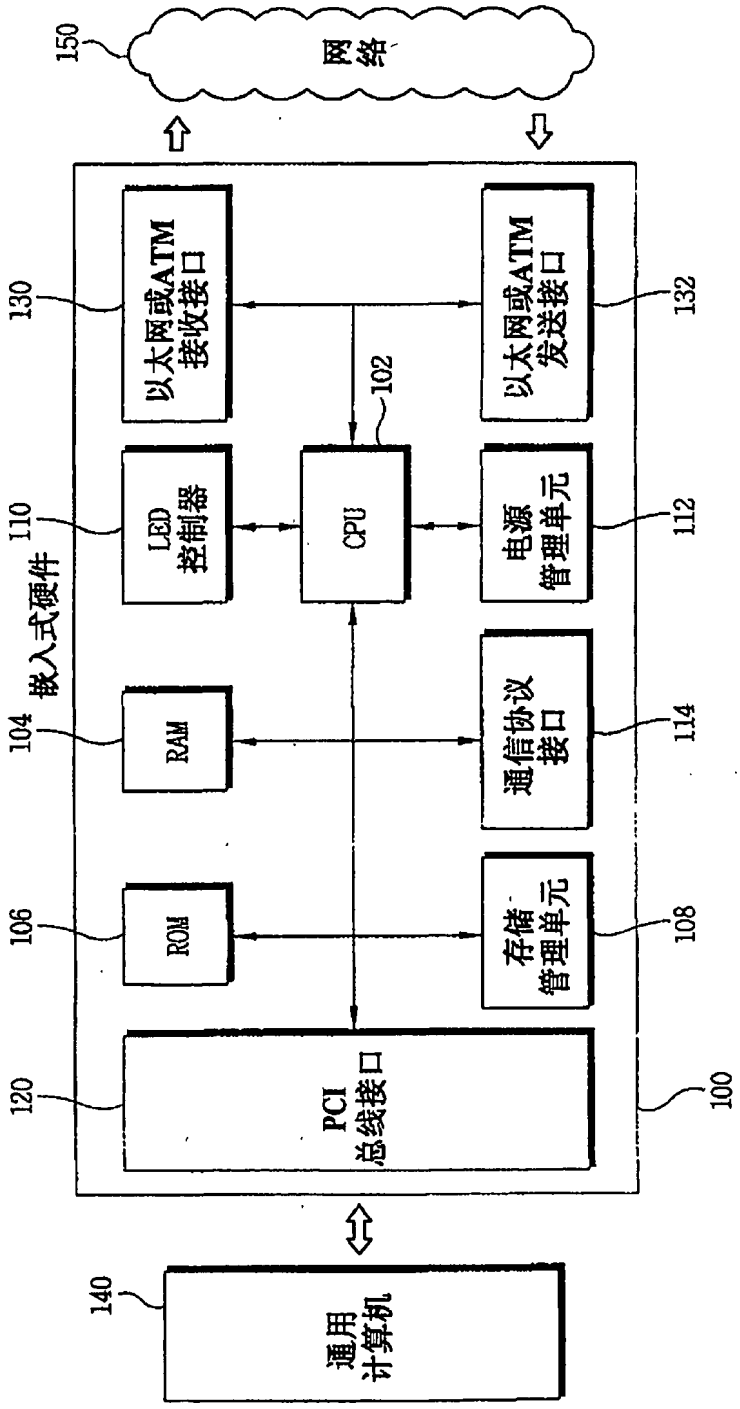

150
网络
嵌入式硬件
130
以太网或ATM
接收接口
132
以太网或ATM
发送接口
102
110
LED
控制器
CPU
电源
管理单元
112
104
RAM
通信协议
接口
114
106
ROM
存储
管理单元
108
120
PCI
总线接口
100
140
通用
计算机

图2

图3

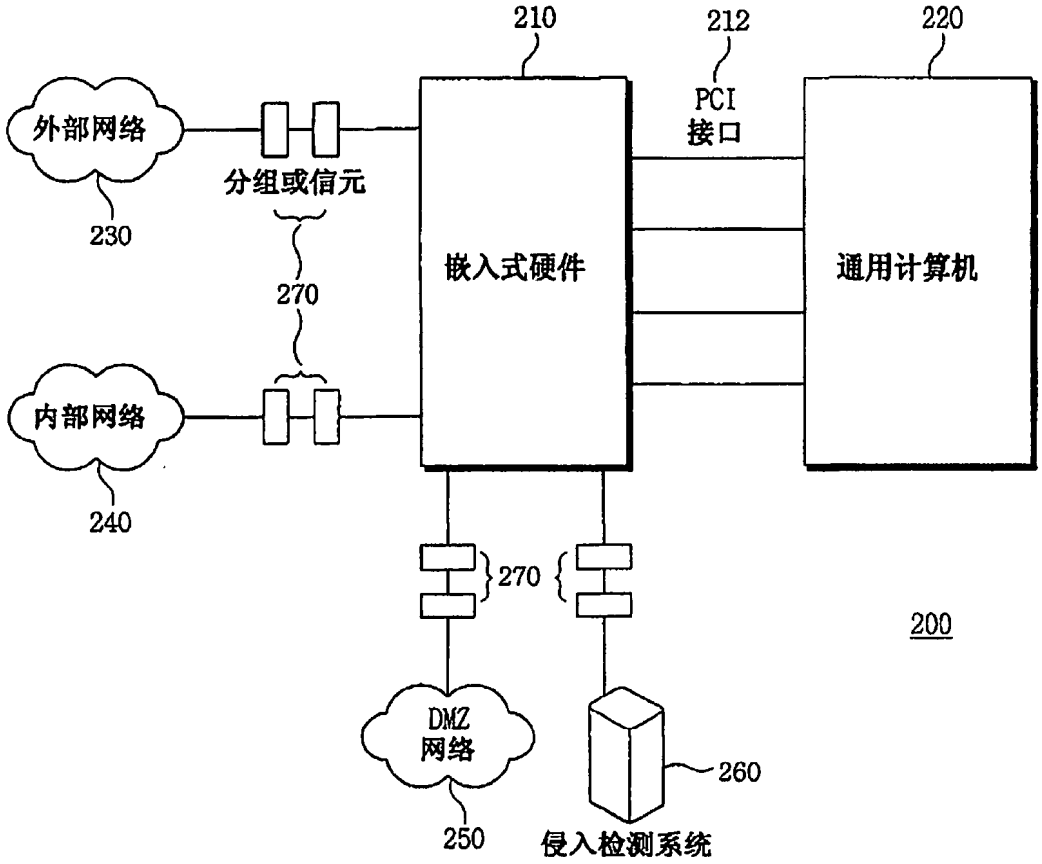
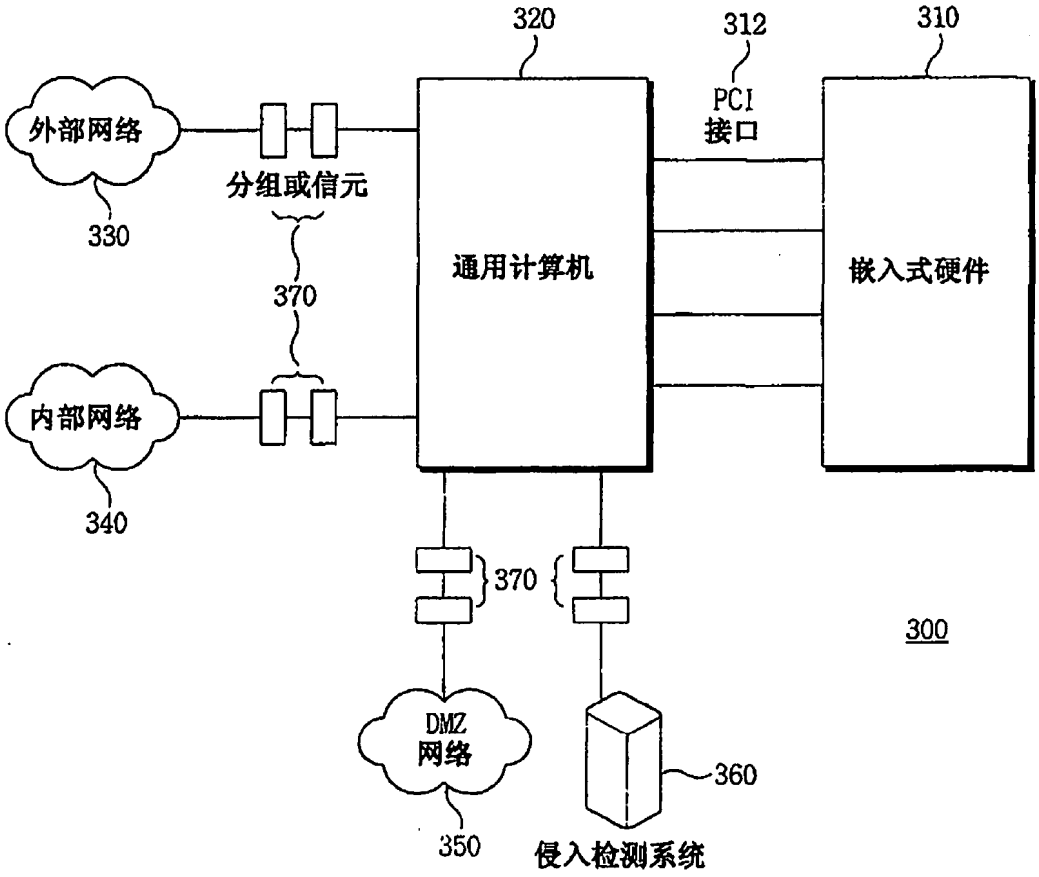

210
212
220
PCI
接口
外部网络
分组或信元
230
270
嵌入式硬件
通用计算机
内部网络
240
270
200
DMZ
网络
260
250
侵入检测系统

图4


320
312
310
外部网络
PCI
接口
分组或信元
330
370
通用计算机
嵌入式硬件
内部网络
340
370
300
DMZ
网络
360
350
侵入检测系统